The Distribution of Privacy Risks

The Distribution of Privacy Risks: Who Needs Protection?

Charles D. Raab

Department of Politics, University of Edinburgh, Edinburgh, Scotland

Colin J. Bennett

Department of Political Science, University of Victoria, Victoria, British Columbia, Canada

It is commonly accepted that the use of personal information in business and government puts individual privacy at risk. However, little is known about these risks—for instance, whether and how they can be measured, and how they vary across social groups and the sectors in which personal data are used. Unless we can gain a purchase on such issues, our knowledge of the societal effects of information technology and systems will remain deficient, and the ability to make and implement better policies for privacy protection, and perhaps for a more equitable distribution of risk and protection, will remain impaired. The article explores this topic, examining conventional paradigms in data protection, including the one-dimensional view of the "data subject," that inhibit better conceptualizations and practices. It looks at some comparative survey evidence that casts light on the question of the distribution of privacy risks and concerns. It examines theoretical issues in the literature on risk, raising questions about the objectivity and perception of the risk of privacy invasion.

Keywords data protection, equity, privacy, risk

INTRODUCTION

This article discusses a relatively neglected topic in the study of information privacy and data protection: the risks posed to privacy by the use of personal information about individuals, the social distribution of these risks, and the ability of laws and practices of data protection systems to ameliorate differentials and thus to promote equality in the distribution of privacy. While threats to information privacy have gained in importance as an issue in the development of an "information society," there is little detailed knowledge about variations in the patterning of privacy and its protection across society. Public policy is therefore less precisely focused than it could be.

An examination of the distribution of privacy risks and protections would not only improve understanding about the effects of information technologies and processes upon society, but might have practical application as well. Privacy advocates and organizations such as Privacy International find it difficult to build coalitions on the very disparate issues to which new surveillance practices give rise. By identifying particularly vulnerable social groups, better knowledge might enhance the protection of their privacy through the activities of general civil liberties organizations or privacy advocates on behalf of such groups, and also affect the political processes through which privacy protection is arbitrated. However, there are many conceptual and empirical difficulties in gaining a purchase on this matter.

Not least of these is the problem of understanding and evaluating risk. Some attempt must be made—if not fully in this article—to come to grips with the way in which hazards are generated by information systems that deal in personal data. This is not only because the concept of risk pervades data protection regulations and rhetoric, and serves as a rationale for the design of protective devices, be they rules, codes of practice, standards, or privacy-enhancing technologies. It is also because the risks associated with the coming of "information society" lend themselves to analysis in terms of social-scientific themes,

Received 2 November 1996; accepted 12 September 1997.

Address correspondence to Charles D. Raab, University of Edinburgh, Department of Politics, 31 Buccleuch Place, Edinburgh, Scotland EH8 9JT. E-mail: c.d.raab@ed.ac.uk

The Information Society, 14:263–274, 1998

0197-2243/98 $12.00 + .00

as Lyon (1994), Gandy (1993), Marx (1988), and others have shown.

The present article explores further some issues that were broached in earlier writing (Raab, 1995).[1] The invisibility of equity issues in data protection is explained and criticized, and the image of the "data subject" is examined with a view to its reconceptualization. In order to gain a closer purchase on the question of distribution, illustrations are cited from the growing body of survey research on privacy, which casts light on public attitudes toward, and knowledge of, privacy risks and privacy protection. The article then looks at the question of risk analysis in order to seek further points of orientation.

DIFFERENTIAL RISKS AND DATA PROTECTION

Regulatory bodies, users of personal data, and individual "data subjects" all play both conflictual and mutually reinforcing parts in data protection systems. However, they cannot easily answer the question, "Who gets what data protection?" Even though a principal aim of data protection policy is to safeguard the privacy of individuals, policymakers and official regulators are less able to achieve their objective to the extent that they only imperfectly monitor the effects that their own and others' activity has upon the privacy of those they aim to protect.[2] The strategies and operations of regulatory bodies may therefore be less effective than they could be. Data users are less able to gauge the impact of processing activities upon their clienteles, and to tailor their own compliance with the principles of data protection. For their part, individuals are less able to develop a critical awareness of their relative place in the distribution of privacy protection, and of their relationship to the systems in which their personal information is used. They, along with political actors and privacy advocates, are also less able to judge how well regulators and data users are protecting privacy.

In more academic terms, our knowledge of the privacy effect of information technology on society will remain one-dimensional without a more finely grained understanding of distributions and patterns. It is often believed that both privacy risks and data protection are unevenly spread across social categories. This assumption is open to fruitful hypothesizing and research, but there are few systematic studies to test it, with a view—in part—to informing regulatory policy and strategy. There is little reliable knowledge of whether the privacy of women, for example, is more often invaded than that of men; nonwhites than whites; poor than rich; old than young; ill people than healthy; and so on. Similarly, the distribution of protection and safeguards is obscure.

Although such dichotomies are far too simple, impressionistic conventional wisdom can be cited on each side of those lines. For example, because the poor more often come into contact with welfare institutions that collect and use their personal details, it is thought that it is they, rather than the rich, who are more vulnerable to the state's misuse of personal information. State surveillance perhaps reinforces existing social stereotypes and categories (Gandy, 1993). On the other hand, it cannot simply be assumed that the poor have less information privacy, in an absolute sense. Those who are further up on the socioeconomic ladder are more likely to be part of the credit-card economy and to be targeted with considerable precision by direct marketers and the private sector in general, exposing them to risks. The Internet is used disproportionately by young, educated, middle-class males. Is it then this social category that is more vulnerable to the abuses of electronic mail or to the surveillance potential of the World Wide Web? With the likely burgeoning of electronic commerce, in what direction will the social—and global—patterning of risk be changed?

It may be easy to speculate that the market economy tends to produce higher levels of surveillance for the educated middle classes, whereas state institutions are more threatening for the poor, women, gays and lesbians, and so on. However plausible, this is guesswork, and there is no adequate investigation of whether variations reflect differences in the way social categories and groups participate in principal sectors of life, such as work, leisure, consumption, education, health care, public order, etc. Yet it is likely that the recording of sensitive information about HIV/AIDS, enforced subject-access requests for criminal or medical records, and the requirement to provide personal details in exchange for social benefits, consumer credit, or employment expose different sections of the population to different privacy risks, and some more than others. But we cannot yet fully map the dimensions of these disparities, devise policies and practices to deal with them, or evaluate the results of the latter. Such differentials may deny equity and have implications for privacy laws and regulations, data protection agencies, and self-regulating industries. While regulators are pressed to "do something about" mail-order firms, credit-card companies, health services, and others, remedying any structured inegalitarian effects of data collection, processing, or communication is very low on the policy agenda.

In sum, despite a few indications of a substantively differentiated approach, data protection discourse and practice have not generally developed in this direction. Laws are based on a general, procedural application of "fair information principles" to all personal data. The distinctions that are introduced do not clearly or primarily aim at achieving equity; nor have they supplanted the main framework of principles, described later. On the other hand, it is neither conceptually nor empirically easy to understand the social distribution of privacy and privacy protection. As will be shown, some studies and reports move in this

direction. However, the difficulty of deriving clear interpretations from their findings reflects the complexities of grappling with different meanings of privacy, varying intersubjective evaluations of risks, and the vagaries of survey research.

THE CONVENTIONAL DATA PROTECTION PARADIGM

Questions concerning the distribution of privacy risks and privacy protection have been obscured by theories and practices that have followed the conventional paradigm for discussions of privacy and data protection systems. The paradigm constructs issues in an adversarial mode—the individual ("data subject") versus the organization ("data user")—within a liberal conception of individual rights (Bennett, 1995). Privacy is seen as the right to be let alone (Warren & Brandeis, 1890) or to control the use of one's information (Westin, 1967). Individuals make claims (or have rights) to the privacy of their personal data against the needs (or rights) of others—typically, organizations—to collect, process, use, and communicate these data. Although some organizations are heavily involved in what is conventionally thought of as surveillance in the narrow sense, such as law-enforcement and order-maintaining agencies, all organizations that use personal data thereby carry out surveillance as construed more widely (Flaherty, 1989).

Writers such as Lyon (1994) and Rule et al. (1980) consider that the conventional paradigm merely manages surveillance, but does not stop its gradual spread. This is partly because the paradigm embodies "fair information principles" that are enshrined in the influential Organization for Economic Cooperation and Development (OECD) Guidelines (OECD, 1981) and in the Council of Europe Convention (Council of Europe, 1981), which are reflected in data protection laws everywhere. An approximate paraphrasing is that they require that data be fairly and lawfully obtained and processed; held, used, and disclosed only for lawful purposes; adequate, relevant, and not excessive; accurate and up to date; not held for longer than their purpose requires; held securely; and accessible to the data subject. But even if followed to the letter, these principles may still legitimate massive personal record-keeping systems. This is because they are largely *procedural*, "due process" principles and do not themselves address *substantive* issues and definitions of privacy (Bennett, 1992, 112). They treat all individuals or citizens alike as abstract "data subjects" without regard to categorical or other empirical variations in their exposure to risks, or their fears.

Some systems leave it largely to individuals themselves to pursue complaints and to seek remedies; this is especially so in the United States. On the other hand, many data-protection systems also involve public-policy initiatives to prevent privacy invasions and to strengthen individuals' control through the provision of regulatory machinery with preventative as well as corrective functions. Thus an official regulatory body can be a potentially powerful third player, arbitrating disputes, monitoring and influencing practice, and contributing to public-policy formation regarding applications of privacy-invasive technologies.

But it may be difficult, and indeed illegitimate, for such a body to pursue social-policy goals within the regulatory routines that follow the conventional paradigm, even where the personal values of data-protection officials incline in this direction, supported by research and pressure-group networks. In particular, there is little that would encourage or legitimize the applicability of criteria related to the social distribution of privacy risks, prevention, and remedies. Officials may have to adhere to administrative and legal norms or political expectations that mainly reinforce an unreconstructed, procedural and abstract, version of the paradigm. It could be argued that equity and other substantive goals are best left to the workings of the political process, rather than to the initiatives of regulators. There may be political demands that data protection's main purpose should be to facilitate the commercial or governmental exploitation of personal data. Regulators may thus be enjoined not to become "activists," but to function only in terms of the paradigm's procedural due process, and to seek "balances."

The question of equity is especially important in view of the prevailing doctrine of "balancing" between the privacy interests of data subjects and the information-processing interests and purposes of data users, however ambiguous this doctrine or however opaque the risk "balancing act" might be (Raab, 1993; Bennett, 1995; Adams, 1995). Given the state of what we may call "regulatory intelligence," discussed later, the practical effect of balancing is to pit the supposed against the known, the Identikit data subject against the drawn-from-life portrait of the data user. This gap might even be widening as more people assume "virtual identities" through their use of the Internet and engage in quasi-social interactions through electronic mail, newsgroups, and the World Wide Web.

In a given instance, a balancing regulator needs to judge whether a data subject's rights (or at least, claims) outweigh the interests of the data user, without bringing to bear a range of particular knowledge about the contending parties. This is a difficult judgement, even in the abstract. But in another sense—and this may be especially so when regulators seek to frame preventative policies, or to influence the development of technologies—balancing requires not only a conception of rights and legitimate interests, but some grasp of the distribution of hazards and fears as well. Because privacy rights do not necessarily prevail over other interests, without such knowledge it may be difficult to argue against data users' persuasive demonstration of

the known and possibly measurable (or costable) harm to their activities if their use of personal data were restricted. This difficulty is especially likely to arise where government policy favors the maximal development of uses and flows of information by itself and others. Regulatory agencies may have little force in a world of public policy that normally gives much less credence to claims on behalf of information privacy, and in which public concern about privacy is only sporadic, weak, or obscurely expressed.

It is true, however, that existing data-protection systems have, indeed, developed a sense of variable risk, but they construe this in terms of different kinds of *data*, and not of different kinds of *persons*. Thus—despite the valid criticism that *any* data might be sensitive, depending upon the context in which it is used—the explicit recognition that some data are inherently sensitive plays a prominent part in data-protection theory and practice. These data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life. These are the "special categories" of data, the processing of which requires special rules under Article 8 of the European Union Directive (European Union, 1995).

In addition, privacy laws normally provide exemptions from, or relaxation of, the rules governing registration, processing or disclosure for classes of data that are regarded as relatively innocuous (e.g., payroll data, household management data). The United Kingdom Data Protection Registrar's thinking about the revision of the registration methods in the British system proposed a simplification predicated on the notion of differential risk across types of data (Office of the Data Protection Registrar, 1996).[3] In some systems, data that are considered especially sensitive, such as physical and mental health data, or genetic information, may even be withheld from the person concerned.

Provided that it can be shown to be sound, the recognition of differentially risky data could be an important conceptual underpinning for a sophisticated regime of privacy protection, and may simplify implementation. However, it only implicitly and inferentially mobilizes an egalitarian principle in counteracting the effects of an uneven spread of social, economic, or other circumstances as they affect exposures to privacy dangers. Equity-oriented protections may therefore only arise *ad hoc* without contributing toward the formation of more explicit, coherent, and frequently used regulatory criteria. These criteria can only be developed by focusing on *persons at risk*, not risky data as such. But there is only an underdeveloped research base that could inform such a perspective, or that would be of interest to social scientists attempting to understand privacy in its social context.

RECONSTRUCTING THE "DATA SUBJECT"

There is a disparity in regulatory intelligence: regulators appear to be more cognizant of the world of data users than of data subjects, and have built this knowledge into regulatory practice. It is rather like medieval maps of the world, where the contours of European lands were more accurately drawn than were the unexplored places beyond the seas. The "detectors" (Hood, 1983) used by policymakers and regulators are more highly developed to acquire information about data users than about those whose data are used; data protection systems are better oriented toward understanding the functional variety of data users than the sociological variety of data subjects and their concerns about invasions of privacy.[4] Sectoral approaches to data protection mean that data users—at least in the more significant industries and sectors such as direct marketing, credit referencing, banking and insurance, the police, and the major public services—are certainly more visible, and their interests more identifiable, than are those of the data subjects.[5]

If they are to act more effectively to protect privacy, policymakers and regulators need a more sophisticated understanding of the variety and attributes of those whose personal data are used. They are currently described in highly abstract terms as "data subjects," "persons," "individuals," "citizens," and "the public." A somewhat clearer picture is gained by reconceptualizing them in terms that map more closely onto the *sectors* of data usage. Sectoral approaches to data protection, which form part of the fine tuning of general rules to specific information practices, facilitate this. For example, banks, shops, and mail-order firms each have "customers," "credit (or loyalty) card holders"; the various social services deal with "clients," "claimants," "patients," etc. Education systems teach "students"; criminal justice systems have "suspects" and "offenders"; political systems involve "voters" and "taxpayers."

Understanding sectoral identities and attributes enables data users, regulators, and data subjects to organize their interactions, and helps to make more precise and predictable one's conduct and one's expectations of others. Claims and rights to privacy protection vary across these categories. Gandy (1993) shows how the "panoptic sort" identifies, classifies, and assesses people as part of surveillance and social control; from a critical perspective, this is the unacceptable practical face of such analyses. Nevertheless, privacy agencies may be able to target their advice and assistance to particular constituencies of subjects based on these more precise identifications. The further development of good information practice would involve data users in knowing more about the privacy concerns of, and risks to, their students, customers, patients, etc.

Sectoral identities of the persons whose data are processed may thus be one route to useful knowledge for better information practices and better regulation.

But if each person is not simply a representative "data subject," neither is he or she simply a customer or taxpayer or voter. It is at least a plausible and researchable hypothesis that the data subject's *social* identities as young/old, rich/poor, healthy/ill, female/male, etc. generate, and help to explain, exposure to varying levels of danger through the processing of personal data in sectors that pose differential risks to privacy and in which the levels of privacy protection vary. Thus it is the *variety of types* of client, patient, etc. that needs investigation, beyond the mere sectoral assignment of the data subject. In terms of the hypothetical data subject that we have just mentioned, the fact that the person is (say) a woman between the ages of 18 and 25, has no higher education, works at a clerical job, and lives in a large city may help to explain the person's privacy circumstances, fears, and perceptions.

From the data subject's viewpoint, the sectoral approach points up the fact that, in daily life, the individual moves through sectoral contexts with different privacy configurations and may have varying attitudes toward these. She tells her doctor what she does not tell her bank. Her tutor does not have to know her financial details, but she cannot withhold these from the tax office. She does not want the benefits office to give her information to her landlord, but would not mind if her solicitor knows her shareholdings. She is more afraid of what her insurance company does with her personal data than what the driving-license bureau does. She thinks that her privacy is more at risk from direct marketers than from her pension fund. She enjoys the convenience of booking theater tickets by telephone with her credit card. Where possible, she may adopt selective strategies for controlling who knows what about herself, and her propensity to raise complaints may vary. She is unaware of many things that are being done "out there" with her data, and worries about some of the possibilities. But she is comfortable with the trade-offs that she makes and the risks that she believes she runs.[6]

This sectoral approach implies that a more sensitive and effective application of data protection principles may be achieved when the data user or regulator knows more about the circumstances and interests of data subjects in different social and economic contexts. It argues for a more precisely tuned appreciation of risks and harms. But the data subject is a *whole person*, with a set of social attributes and variable preferences, and cannot simply be represented as an aggregation of sectoral roles. This way of looking at it runs sociological variables across the sectors to produce a two-dimensional view, which is at least better than a one-dimensional view.[7] But the routinely recorded administrative statistics of data protection agencies have not normally been disaggregated sufficiently to allow for a more nuanced understanding, and for recombination in order to address the "whole person" question across sectors and social categories. Yet there is useful public-opinion survey evidence that provides a starting point for further investigation, insofar as it provides a more rounded sociodemographic view of the public. What does it indicate?

SOME SURVEY EVIDENCE

Only a few relevant research findings can be adduced here. In general, surveys bear out the generalization that levels of privacy concern are relatively high and are broadly similar across countries (Bennett, 1992, 37–43). While the definition of "privacy" may be ambiguous, surveys reveal perceptions of risk and attitudes toward particular aspects of data protection. They also tap the dimensions of fear and trust as well as showing the extent to which privacy is valued and its protection is seen as desirable. Let us look selectively at some of them.

Since 1986, the UK Data Protection Registrar has reported general findings among "members of the public," although these statistics are not broken down in order to show important demographic variations. Survey results fluctuate from year to year, sometimes reflecting the effects of advertising campaigns. In 1994 (Data Protection Registrar, 1994)[8] it was reported that protecting people's rights to personal privacy was a "very important" issue for 66% of the sample of 1,000 persons. Seventy-two percent were "very" or "quite" concerned about the amount of information that is kept about them by various organizations. Concern about the keeping of information without their knowledge was particularly high, ranging from 94 to 59%, with respect to details about savings, earnings, court judgments, credit ratings, one's visitors, and medical history. The proportions were lower with regard to education and job history, what one buys, club membership, TV viewing, newspaper reading, and age, ranging from 38 to 13%.[9] Doctors and the National Health Service were the organizations that respondents trusted most with their data (88%), and mail order companies the least (22%). Interestingly, this same rank ordering was found when questions about trust in different organizations were asked in Australia (Australia, Privacy Commissioner, 1995, 12) and in Canada (Ekos Research Associates, 1993, 20).

Although the British public were apparently very concerned about privacy, few respondents knew much about their rights. Only 47%—with prompting—were even aware of the Data Protection Act, although this was a significant increase from the 38% of the previous 2 years. Even smaller proportions of the "aware" minority knew what functions the act performed.[10] But the Registrar's published data are not disaggregated by sociodemographic

variables, so we do not know who fears what, who trusts whom, and who knows what about their legal entitlements. A similar lack of awareness about privacy rights was discovered in Australia (Australia, Privacy Commissioner, 1995).

Some informative findings about social distributions of attitudes toward the provision of personal information are available in research conducted by outside organizations. In Britain, a survey carried out by the Henley Centre with the sponsorship of the Direct Marketing Association disaggregated findings by age, social class, and industrial sector. It identified consumers' fears about exclusion, inaccuracy, the passing on of information, and technology. Among the findings were that the fear of being labeled by companies was strongest among older and poorer people, but was a majority response in all categories. Inaccuracy was feared by the vast majority—89% overall; 87% opposed the passing on of information to other companies, and there was also a widespread fear of information technology's capability of linking data and compiling dossiers (Henley Centre, 1995, ch. 4).

The Harris–Equifax surveys in the United States, conducted by a leading credit referencing company in connection with Alan Westin, have provided data in general as well as in specific fields and sectors. The first in the series (Equifax, 1990) was a survey of over 2,000 consumers as well as a smaller number of data-using business executives. In 1991, Westin's analysis drew a distinction between "privacy fundamentalists" (25%), "the unconcerned" (18%), and "the pragmatic majority" (57%). "Fundamentalists" were the most distrustful of organizations and concerned about the use of data; at the other end of the scale, the "unconcerned" did not worry and valued consumption benefits and public order over their privacy. The "pragmatic" had more subtle and discriminating views concerning particular organizations, practices, and values (Harris–Equifax, 1991, 6–7).[11]

The 1994 survey (Equifax–Harris, 1994) of about 1,000 persons employed categories of age, education, race, sex, region, type of community, political philosophy, and household income.[12] It found that 84% of Americans were "very" or "somewhat" concerned about privacy threats. This was the highest percentage found in a number of surveys going back to 1978, with 71% of blacks "very" concerned, as compared with only 48% of whites. Those aged between 18 and 24 were less concerned than those aged 50–64, and those earning less than $15,000 per year were far more concerned than those earning over $75,000. College graduates were much less concerned than those who had never completed high school. In general, the arguably related variables of race, income, and level of education seem to explain variations in attitudes toward the use of personal data across a wide range of contexts and issues that include the use of social security numbers, a proposed national identification system, medical research, and utility services.

It is evident that trust plays an important part in individuals' perception of risk. Doctors and nurses were trusted with personal data far more than were mail-order companies, and in about the same proportions as in Britain. But the survey found that individuals' level of distrust in government and in technology—particularly high in the United States, and increasing over the years—correlated with their attitudes on privacy issues.[13] Comparisons with equivalent Canadian data have revealed similar correlations, perhaps in contrast to the conventional wisdom that Canadians are more trustful of government institutions than are Americans (Harris–Equifax, 1992, ix).

However, even some of the very distrustful were found among those who were prepared to accept particular uses of personal information on condition that safeguards were provided in the form of laws, remedies, and voluntary fair information practices applied by data users. The survey showed that willingness to change from opposition to acceptance was stronger among the demographic groups that were most worried about privacy threats: "These include African-Americans; respondents with less than high school education; Southerners; suburbanites; and persons 40–49 years of age" (Equifax–Harris, 1994, xix). Findings of this kind are particularly interesting because they suggest that the perceived level of risk cannot be taken as an unexplained prior condition, but interacts with safeguards and is influenced by the latter's availability.

A survey concerning health information in the United States showed that levels of concern for privacy differed according to income, gender, age, geographical region, level of education, and other variables (Harris–Equifax, 1993). Detailed comparisons of figures across survey years cannot be discussed here, but Westin's interpretative essay gives the following overview:

> Blacks are generally among the higher concerned groups on medical- and other privacy issues. Harris–Equifax surveys have shown low-income, low-education, and minority-racial groups to be among the most highly concerned about general privacy threats, violations of employee and consumer privacy rights, and government invasions of citizen privacy in law enforcement and social-program administration. It is not surprising, therefore, to find these sectors of the public scoring "high concern" on medical-privacy issues in the 1993 survey. (Harris–Equifax, 1993, 15)

Westin also points out that respondents with the least and the highest levels of education and of income were highly concerned to comparable degrees on many questions. This was surprising because other surveys have shown that high-income, well-educated people are not generally highly concerned about privacy. Westin's suggested explanation is that these groups:

> are among the heaviest users of mental health services and also report having their medical information improperly disclosed at rates much higher than the public. It may be that such respondents feel capable of defending their informational interests quite well in the employment and consumer contexts, and feel a part of the governing elite as far as general privacy concerns are involved. But, their use of mental health services and their adverse medical confidentiality experiences make them feel sensitive—and vulnerable—when medical and health information is involved. (Harris–Equifax, 1993, 15)

The survey is noteworthy for its focus on data practices, and on the attitudes of both the public and "leaders," in a specific and particularly important sector. Westin's interpretation is also especially germane in view of what has been said earlier about sectoral approaches and about the variations in the empirical patterning of individuals' participation in, and exposure to the privacy dangers in, informatized areas of social, economic, and governmental life.

Another survey, the 1993 Canadian Privacy Survey, also revealed group variations in fear of serious privacy invasions (Ekos Research Associates, 1993), but puts a somewhat different interpretation on them: one that is related more to powerlessness rather than to the degree of inclusion in information-using (and -misusing) systems. In general, the elderly, the less educated, women, and Francophones expressed higher levels of concern. But the authors see a "class cleavage in the nature and impact of privacy issues" (Ekos Research Associates, 1993, iii). They argue:

> For those in the less powerful and less privileged classes, . . . powerlessness may be combining with a growing disillusionment with Government and other institutions, to produce a generalized fear. . . . At the same time, their economically marginal positions render them less capable of identifying and responding to these problems. For example, they are least capable of affording some of the new technologies designed to minimise privacy threats. They are also least likely to be subject to the irritants of marketing intrusions, since they are not attractive marketing opportunities. . . . More privileged members of society, on the other hand, understand and experience privacy issues in a fundamentally different way. As consumers, they are the more likely users of the new information technologies . . . they endure the majority of telemarketing and charitable agency intrusions. Finally, they are also more interested in and capable of affording new privacy protection services. (Ekos Research Associates, 1993, iii)

The Canadian report distinguishes among persons with different levels of concern over privacy, in terms of an exotically labeled fivefold typology based on factor analysis: "fearful regulators," "extroverted technophobes," "guarded individualists," "open pragmatists," and "the indifferent" (Ekos Research Associates, 1993, 34–38). The relationship between these divisions and sociodemographic characteristics of members of each category points up the complexity of privacy as a socially distributed value, and shows that generalizations about (say) women, the poorly educated, or the young cannot be made with confidence. The report plots the typological groups against seven sociodemographic variables, but there are no indications of statistical significance among the differences that are shown (Ekos Research Associates, 1993, 64).

Most Canadians do not appear to know how to handle privacy problems, according to this survey. Sixty-one percent would not know whom to turn to, although this varied by age (the older, the more knowledgeable) and region (Francophones felt better able). Knowledge of how technologies affect privacy was somewhat more widespread, but social-group differences were small. Awareness of the possibility for formal recourse was low, but again it was higher among Francophones. There was a strong desire for government legislation, although other protective strategies received support as well.

Three further illustrative surveys can be cited. A Dutch enquiry reported the results of a privacy questionnaire in terms of a range of variables including religious and political affiliation and several employment categories (Holvast et al., 1989). An international European survey found that more women than men appear to be worried about leaving electronic tracks on information networks. Levels of concern correlate closely with age level of education across all countries. Awareness of data protection laws is variable and often low, although there are very high proportions in all countries—above 90%—who attach a high level of importance to privacy protection and think the European Union should ensure this (International Research Associates, 1997). In a Hungarian study, geographical, educational, age, and occupational factors were taken into account in analyzing responses to a questionnaire investigating issues concerned with the administrative use of personal data, including trust and safeguards (Székely, 1991). One finding was that persons' sensitivity about medical history, income, finances, family life, and personal past and future plans was related to age. Those over 66 were less demanding of information privacy; an explanation is:

> Elderly people, especially single ones, have to rely on other people's help and on medical and social services more intensively. . . . For all of this they have to give more information about themselves and to disclose an increasing number of dimensions of their private lives. To this is added their generally reduced incomes, and beyond a certain degree they are compelled to draw attention to this fact. (Székely, 1991, 19)

Sensitivity was found to be highest among the young, who are thought to have a greater need for "informational self-determination" on many categories of information. The less educated were also less sensitive; this is attributed to the lower levels of privacy in their families and communities, and to the lower frequency of their contacts with

officialdom in which data might be disclosed. They also are considered to be less knowledgeable about information processing and use (Székely, 1991, 19).

One aim of the enquiry was to identify and explain the circumstances of a social group who were particularly aware of the need for data protection and who demanded information privacy and autonomy. A subsample was identified. Its members were

> somewhat better informed, . . . are more interested in the fate of their data, pay more attention to the differences between named and anonymous data processing, are bothered more by compulsory provision of data, and more strongly oppose the establishment of interconnection among registrations. . . . they place safety before comfort, prefer decentralised to centralised registration, and are suspicious about the computerised processing of personal data. Accordingly, they more strongly oppose an expansion of [State Office for Population Registering] activities, call for more information about their data, and almost 100 per cent of them oppose the selling of their personal data for various information services. (Székely, 1991, 37)

Contrary to the conventional wisdom that would suppose them to be politically active and technologically sophisticated young Budapest intellectuals, it was found that they were not significantly different from the whole sample in terms of the full range of sociodemographic variables. This is believed to reflect the nature of Hungarian society at the time of the survey, in which the opportunity for information privacy had not been available, and in which consciousness of data protection could be traced to "familial, religious, cultural and other traditions" (Székely, 1991, 37) rather than directly to the other variables. This configuration of high privacy awareness and desire is seen as constituting a new dimension in society.

PRIVACY RISKS REVISITED

The preceding discussion has concerned perceptions of privacy threats and of safeguards or protective measures that might mitigate the risks posed by personal information processes. In terms of its contribution to knowledge and policy, the state of research is somewhat encouraging, especially where surveys have used sectorization as well as sociodemographic breakdowns as analytical dimensions. Levels of knowledge and awareness of privacy threats, technological processes, and the administrative use of data have been ascertained, and the dimension of trust/distrust has been singled out as important, particularly in relation to perceived needs or demands for better privacy protection.

Evidence of this kind is highly relevant. It shows who feels threatened by privacy invasions, who knows about data protection, and who would be reassured by safeguards on the processing of personal data. These findings should ideally be run against actual patterns of involvement of different categories of data subject with various sectors of data usage, as does the Equifax–Harris (1996, 15–22) comparison among credit-card holders, direct-mail purchasers, and Internet users. More precise information might be difficult to obtain, but not impossible. Estimates might be available from data users whose knowledge of their clientele or customers includes relevant socioeconomic or other characteristics. Therefore—and especially if the question of equality is to be addressed—closer attention should be paid to differences that might give a purchase on systematic demographic variations that might help us to understand why some people feel more exposed than others. To a degree, some surveys already do this, providing explanations of attitudes. Important variables in the Equifax–Harris surveys, for example, are whether the respondent has or has not been a victim of a privacy invasion, and the relative importance of the consumer's own personal experiences with business firms in shaping attitudes.

However, an important limitation is that the results do not provide much information on the distribution of *data protection* as a specific service or regulatory function, or on the efficacy of data protection systems in coping with, or ameliorating, risks and fears. They cannot coherently answer the question, "Who gets what data protection?" Looking at it through this end of the telescope, the available knowledge about how privacy protection laws and systems work does not easily relate to the circumstances of particular individuals or groups, although it gives some insights into this. It was argued earlier that regulators have a clearer understanding of data users' practices than of data subjects. Moreover, these patterns of risk, protection, and perception may vary by sector, by country, and by type of person.

Thomas's (1928) aphorism, that situations defined as real are real in their consequences, should not leave us too upset if we cannot get very far beyond the plane of popular perceptions and attitudes toward privacy risks, and plausible explanations of them. Policymakers and privacy-regulating bodies, as well as data users themselves, need to respond to these fears, distrusts, and demands, however "unrealistic" these may be thought to be by those who would try to calculate risks. In our attempt to understand policy processes, we may then note that the organizational and regulatory response to opinions and attitudes, and not necessarily to what some would construe as "objective" fact, is a key component in shaping policy and in the political construction of privacy as a problem.

Still on the plane of perceptions and attitudes, the evidence shows that sensitivity to privacy issues does vary to some extent across the social spectrum. What it does not show is whether these differences correspond to differences in actual exposure to risk, although, as we have seen, there are plausible exposure-related reasons why the

old, the ill, etc. feel vulnerable. It might be argued that we need some way of assessing "real" hazards, both generally and for different groups or categories of people; otherwise, we cannot say whether they—or government, politicians, privacy advocates, etc.—are under- or overreacting, pandering to popular fears, negligent in the face of threats, or tailoring policy appropriately.

There are parallels here to crime and the fear of crime—the "law and order" agenda—and connections with the problem of evaluating the "adequacy" of data protection (Raab & Bennett, 1996b). There are also issues concerning false consciousness and the propriety of "educating, agitating, and organizing" the public, engaging them in the political arena to gain better privacy protection, all on the basis of unfalsifiable assumptions. But conversely, there are also ethical issues about keeping people uninformed and therefore quiescent about dangers to which they may be exposed. Exaggeration of the risks or individuals' lack of concern for their privacy are both worrisome, as well as being data for sociological study.

Where do these issues lead us? Do we need, and can we obtain, "objective" knowledge of the variable hazards to which people are exposed through the collection and use of their personal details? Are we—whether inevitably or only currently—less able to show the distribution of privacy risk across society than we might be, say, to demonstrate the distribution of environmental hazards or physical safety? Is the attempt to understand the pattern of inequality and to determine more precisely how far we are from the *equal* protection of personal information doomed to failure? Are we left only with what people think or fear, rather than some "harder" reality? And if so, what then?

These are large questions that confront not only the state of the art of empirical research but the whole status of "objectivity" and "rationality" in social science. In particular, they are at the heart of contemporary controversy and debate in the literature on risk analysis and risk assessment.[14] Some take the view that the expert, objective determination of risk is the only reliable knowledge, and that lay people's subjective views—where they differ—should be discounted as error. This view has been challenged, and may even be superseded, by the view that "expert" knowledge is also to a degree subjective, value-laden, and dependent upon judgment. Because the distinction between the two forms of knowledge cannot be firmly established, there is no valid reason to exclude perceptions in assessing and managing risk (Royal Society, 1992, ch. 5; Slovic, 1987, 1997). As Beck observes, "The scientific concern . . . relies on social expectations and value judgements, just as the social discussion and perception of risks depend on scientific arguments . . . scientific rationality without social rationality remains *empty*, but social rationality without scientific rationality remains *blind*" (Beck, 1992, 30; emphasis in original).

On the other hand, risk management and policy are more complex given the diversity of risk perceptions across a population. Resolving these differences is a matter of political as well as scientific choice; the acceptability of a risk has to be answered in terms of "to whom, . . . when, and under what circumstances?" (Royal Society, 1992, 92). The policy and administrative dilemma is "how, in the face of such plurality, societal decisions about risks may be made that are both equitable, and in some way in the interests of all" (Royal Society, 1992, 124). There are group differences in risk perception that appear to be associated with individuals' membership in, or identification with, different groups or sociocultural categories and therefore with adherence to different beliefs and norms (Royal Society, 1992, 108). Although no specific research on privacy risk perception has been done to test this or other findings, risk research generally is persuasive in concluding that "purely psychological, individual-based analysis can account for only a part of risk perception and risk behavior" (Royal Society, 1992, 112). The individualist perspective of data protection and of many existing surveys tends to obscure these matters.

Recent writings on risk offer further helpful insights. Beck (1992) has noted the relationship between the paradigm of industrial or "class" society and the new paradigm of "risk society," which also involves issues of inequality. He recognizes disparities in the distribution of risks, and talks about "social risk positions" (Beck, 1992, 23) that follow class inequalities, but that might take a different path that rebounds on those who produce or gain from risks. He has particularly in mind pollution, ecological risks, etc., but as his argument thereby comprises situations that ignore national borders and are global, the case of perssonal information flows might be germane as well.

Especially interesting is his point that, with risk, "[k]nowledge gains a new political significance" (Beck, 1992, 23), and we are thus pointed toward the development of "a sociological theory of the origin and diffusion of *knowledge about risks*" (Beck, 1992, 24; emphasis in original). This is relevant to privacy risks because, as has often been pointed out, the lack of transparency of data processing means that individuals are not often able to understand what happens to their personal details once they are collected, or even to know when in fact they are being collected. This situation may breed rumor and thence fear, which is often registered in survey responses. Newspaper "horror stories" about privacy invasions and misuse of data, as well as personal or bar stories about these, and daily evidence of surveillance by means of closed-circuit cameras, may validate and shape the individual's perception of privacy threats, but they may not be accurate measures of the risks to which people are subjected.[15]

Yet these perceptions cannot be brushed aside by a "scientistic" determination of risk; they are real, and real in

their consequences. Beck argues:

> [R]isk determinations are an unrecognized, still undeveloped symbiosis of the natural and human sciences, of everyday and expert rationality, of interest and fact. They are simultaneously neither simply the one nor only the other. They can no longer be isolated from one another through specialization, and developed and set down according to their own standards of rationality. They require a cooperation across the trenches of disciplines, citizens' groups, factories, administration and politics, or—which is the more likely—they disintegrate between these into antagonistic definitions and *definitional struggles*. (Beck, 1992, 28–29; emphasis in original)

We may infer from this that it is not futile to investigate actual risk patterns, seeking estimates of the probabilities, magnitudes, and distributions of risk according to a range of sociodemographic variables. It is also very worthwhile to investigate, as far as possible, the privacy implications of policies, information systems, and business processes in government and the private sector.[16] But we should not expect incontestable results that would resolve issues, settle all conflicts between data users and data subjects, or provide data protectors with reliable strategies. Adams holds that science cannot resolve disagreements about risk, "[b]ecause people are constantly responding to their circumstances, and thereby constantly altering each others' risk-taking environments . . . the future is constantly being reshaped by people's perceptions of it. Science has no firm ground on which to stand" (Adams, 1995, 194).

Drawing upon a typology derived from cultural theory,[17] Adams's (1995) distinction among types of perspectives on risk bears resemblance to some of the categories of privacy stances that we have seen in some of the survey research. Briefly, "individualists" play down risks, oppose regulation, and leave risk decisions to the market and individual discretion. "Hierarchists," on the other hand, seek the authoritative, scientific management of risk from the top down, with regulation grounded in "research to establish 'the facts' about both human and physical nature" (Adams, 1995, 41). "Egalitarians" perceive risks but are prudent and cautious, sometimes favoring regulation but sometimes opposing it on grounds that it inhibits other desirable behavior; they seek cooperation in reducing risk. "Fatalists" see an unpredictable world that they cannot affect, and therefore play no part in arguments about risk. Because they argue from different premises about the nature of the world, they disagree about matters that are fundamental to the question of risk, such as its acceptable level (Adams, 1995, 59). The decisions they take—the "balancing act in which perceptions of risk are weighed against propensity to take risk" (Adams, 1995, 15)—are filtered through their different cultural outlooks to produce different conclusions.

One consequence of this cultural model for our discussion of knowledge about "real" risks is that the outlook of the "hierarchists" is not privileged in the sociocultural construction of risk. Their resource—scientific research—may be no more a trump card than are privacy "rights." If the knowledge they possess about risks is deficient for the purpose of regulation, the call for "good science" is misplaced, in Adams's view:

> On occasion science may succeed in solving a problem by the discovery of new agreed "facts" which can serve as a basis for consensual action. . . . But in such cases science has simply removed the issue from the realm of risk; it has not solved the problem of how to proceed in the absence of agreed facts. (Adams, 1995, 195)

Douglas and Wildavsky (1982) make a similar point when they argue that risk assessment needs to take account of both subjective and objective aspects of problems, but that it would require settled societal values underpinning adequate methods of discovering facts and of making political decisions:

> That would be a trusting world, but it is not the one in which we live. There is neither agreement over appropriate methods to assess risks nor acceptance of the outcomes of public processes. Advanced techniques of risk assessment arrive in the very scene in which they are the least appropriate. (Douglas & Wildavsky, 1982, 68)

CONCLUSION

A firm stance on these issues cannot be taken in the absence of further investigation of privacy risks and perceptions. In the final analysis, however, although "good science" may not be able to sort out risk problems, *some* science may be better than no science, and increments of knowledge about exposures to privacy hazards and their distribution may help to put the claims of both the alarmist and the complacent into perspective. But little of such knowledge is available. Scientific research on issues such as road safety and environmental pollution—the usual cases in point in the risk literature—is far further down the path, even if that path is a false trail and an "objective" determination of risk, complete with cost-benefit analysis, is dangerously misleading. Privacy risks and their distribution have not yet enjoyed a widespread, evidenced discourse that might reveal where the areas of agreement and disagreement lie among protagonists with different outlooks, what "facts" can be accepted, what the range of risk probabilities and magnitudes might be, and what is plausible or far-fetched in regard to who gets what privacy.[18]

Therefore, survey and other evidence, and debates about the findings, might well suggest strategies for coping more effectively with risks and fears thrown up by information technology and its applications, and with disparities among social groups and categories in the protection of their personal information. These strategies could be

employed not only by regulatory "hierarchists" but also by "pragmatists" or "egalitarians" in pursuit of their various objectives. "Individualists" or the "unconcerned" might even find that some research casts light on the feasibility of their position by showing the effect of certain solutions, such as privacy-enhancing technologies and market-based initiatives. "Fatalists," as Adams (1995) shows, sideline themselves in arguments of this kind, but better knowledge might show how their privacy, too, can be protected, as of right.

Debates about privacy are, in large part, debates about politics. Beyond research and strategies, in considering the distribution of privacy risks and of privacy protection, Douglas and Wildavsky's view should be borne in mind:

> Knowledge of danger is necessarily partial and limited: judgments of risk and safety must be selected as much on the basis of what is valued as on the basis of what is known. . . . Science and risk assessment cannot tell us what we need to know about threats of danger since they explicitly try to exclude moral ideas about the good life. . . . If we agreed on what polity we desired, we could consider what risks would be worth facing for establishing it. (Douglas & Wildavsky, 1982, 80–82)

NOTES

1. Previous versions were given at the ETHICOMP96 Conference in Madrid, November 1996 (see Raab & Bennett, 1996a) and at the Conference on Risk, City University, London, June 1997. The authors are particularly grateful for comments from Paul Anand, Dag Elgesem, Jeroen van den Hoven, Simon Rogerson, and Paul Slovic.

2. The general problem of the measurement of the quality of data protection has been dealt with elsewhere (Raab & Bennett, 1996b).

3. "We propose to distinguish between sensitive and non-sensitive data, to focus on a list of 'sensitive' purposes, and discriminate between sensitive and non-sensitive data, sources and disclosures. . . . There will inevitably be different views as to which uses of data are particularly sensitive. . . . It is easy to make a case for any data to be classed as 'sensitive' . . . in many cases the sensitivity of data relates to the purpose for which it is held and its possible disclosures (Office of the Data Protection Registrar, 1996, paras. 4.6, 8.1, 9.1).

4. Interesting exceptions can be noted, illustratively. For example, there have been Australian surveys "identifying the privacy concerns of Aboriginal and Torres Strait Islander people in the Northern Territory," and examining the difficulties faced by people with disabilities in regard to access to medical records (Human Rights Australia, 1995, 9).

5. This does not necessarily mean that data users are particularly influential in the policy process, or that all data users are equally well-placed as policy actors. However, it is arguably the case that, in general, they are more able to mobilize for these purposes than is the public at large, as in other fields where citizens or consumers as such are among the less well-organized and less sophisticated political actors. It is, however, an open question whether any disparities in influence are reinforced by the disparity in regulatory intelligence.

6. On the question of individual choice, see Elgesem (in press).

7. A third dimension might be chronological, registering the improvement or worsening of risk-and-protection positions over time for categories of persons and within sectors.

8. The 1994 figures are shown here because they were more detailed than those published in subsequent years. No survey results were published in the Registrar's 1995 Annual Report.

9. No question was apparently asked about information concerning driving habits, video-surveillance data, or records of telephone calls—areas of data capture and processing that are becoming increasingly important.

10. Although the figures reported for 1997 (Data Protection Registrar, 1997, Appendix 8) are not directly comparable, public awareness (especially following advertising) has increased considerably to roughly two-thirds. But perhaps more disturbing is the 1994 finding that 40% of computer-record-holding small businesses, and 20% of large businesses, were unaware that they had to register their holdings with the Registrar. Ten years after the passage of the Act, only 43% and 72%, respectively, were aware that the act conferred rights on individuals. These proportions have varied over the years, and improved in 1997 following a media campaign.

11. The Equifax–Harris figures for 1996 were 24% "fundamentalists," 16% "unconcerned," and 60% "pragmatists" (Equifax–Harris, 1996, 13). The survey by the Henley Centre found 9% "fundamentalists," 8% "unconcerned," and 80% "pragmatists," although these proportions were only considered indicative (Henley Centre, 1995, 87–88).

12. Whether the categories used in such surveys are the relevant ones for an understanding of inequalities, whether the categories define actual social groups, and whether groups identified in other ways, including self-identification, would provide a better basis for analysis of inequalities are important methodological issues that cannot be discussed here.

13. "The higher a respondent's distrust, the more he or she is concerned about threats to privacy, opposed to new uses of personal information (especially through information-technology applications), and in favor of legal and regulatory bans or controls on uses of personal information by business or government" (Equifax–Harris, 1994, xii).

14. See, for example, the Royal Society (1992).

15. Cf. the discussion of "risk communication" in the Royal Society (1992), ch. 5.

16. See the discussion of privacy impact analysis in Bennett (1995, ch. 6) and the literature cited therein; also see Stewart (1996).

17. See also the Royal Society (1992, 112–114) and the literature cited therein.

18. See, however, the philosophical discussion by Elgesem (1996) of privacy risks, their justification, and their acceptability with particular reference to registers of medical information for epidemiological research.

REFERENCES

Adams, J. 1995. *Risk*. London: UCL Press.

Australia, Privacy Commissioner. 1995. *Community attitudes towards privacy*. Canberra: Human Rights Australia.

Beck, U. 1992. *Risk society*. London: Sage.

Bennett, C. 1992. *Regulating privacy*. Ithaca, NY: Cornell University Press.

Bennett, C. 1995. The Political Economy of Privacy. Hackensack, NJ: Center for Social and Legal Research, unpublished paper.

Council of Europe. 1981. *Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [includes Treaty No. 108]*. Strasbourg: Council of Europe.

Data Protection Registrar. 1994. *Tenth Report of the Data Protection Registrar June 1994*. HC 453, Session 1993–94. London: HMSO.

Data Protection Registrar. 1997. *The Thirteenth Annual Report of the Data Protection Registrar June 1997*. HC 122, Session 1996–97. London: The Stationery Office.

Douglas, M., and Wildavsky, A. 1982. *Risk and culture*, Berkeley, CA: University of California Press.

Ekos Research Associates. 1993. *Privacy revealed*. Ottawa: Ekos Research Associates, Inc.

Elgesem, D. 1996. Privacy, respect of persons, and risk. In *Philosophical perspectives on computer-mediated communication*, ed. C. Ess, pp. 45–56. Albany: State University of New York Press.

Elgesem, D. In press. Data protection and the limits of centralized risk assessment. In *A reader in information ethics*, eds. S. Rogerson and T. Bynum. Oxford: Blackwell.

Equifax. 1990. *The Equifax Report on Consumers in the Information Age*. Atlanta, GA: Equifax, Inc.

Equifax–Harris. 1994. *Equifax–Harris Consumer Privacy Survey 1994*. Atlanta, GA: Equifax, Inc.

Equifax–Harris. 1996. *The Equifax–Harris Consumer Privacy Survey 1996*. Atlanta, GA: Equifax, Inc.

European Union. 1995. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*. L281/31, 23/11/95.

Flaherty, D. 1989. *Protecting privacy in surveillance societies*. Chapel Hill, NC: University of North Carolina Press.

Gandy, O. 1993. *The panoptic sort*. Boulder, CO: Westview Press.

Harris–Equifax. 1991. *Harris–Equifax Consumer Privacy Survey*. Atlanta, GA: Equifax, Inc.

Harris–Equifax. 1992. *The Equifax Canada Report on Consumers and Privacy in the Information Age*. Ville d'Anjou: Equifax Canada.

Harris-Equifax. 1993. *Health Information Privacy Survey 1993*. Atlanta, GA: Equifax, Inc.

Henley Centre. 1995. *Dataculture*. London: Henley Centre for Forecasting, Ltd.

Holvast, J., van Dijk, H., and Schep, G. 1989. *Privacy Doorgelicht*. Onderzoeksrapport No. 71.'s-Gravenhage: SWOKA.

Hood, C. 1983. *The tools of government*. London: MacMillan.

Human Rights Australia. 1995. *Privacy Commissioner—Seventh Annual Report on the Operation of the Privacy Act*. Canberra: Australian Government Publishing Service.

International Research Associates. 1997. *Information Technology and Data Privacy: Report Produced for the European Commission*. Brussels: INRA.

Lyon, D. 1994. *The electronic eye*. Cambridge: Polity Press.

Marx, G. 1988. *Undercover: Police surveillance in America*, Berkeley, CA: University of California Press.

Office of the Data Protection Registrar. 1996. *Heading for the Future: A Consultation Paper—A Proposal for Revision of Registration Methods under the Data Protection Act 1994*. Wilmslow: Office of the Data Protection Registrar.

Organization for Economic Cooperation and Development. 1981. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD.

Raab, C. 1993. The governance of data protection. In *Modern governance*, ed. J. Kooiman, pp. 89–103. London: Sage.

Raab, C. 1995. Equality and privacy: Who gets what data protection? In *Privacy disputed*, eds. P. Ippel, G. de Heij, and B. Crouwers, pp. 111–122. Den Haag: SDU.

Raab, C., and Bennett, C. 1996a. Distributing privacy: Risks, protection and policy. In *Proceedings of ETHICOMP96—Values and Social Responsibilities of Computer Science*, ed. P. Barroso, pp. 336–350. Madrid: Universidad Complutense de Madrid.

Raab, C., and Bennett, C. 1996b. Taking the measure of privacy: Can data protection be evaluated? *International Review of Administrative Sciences*, 62(4):535–556.

Royal Society. 1992. *Risk: Analysis, perception and management*, London: The Royal Society.

Rule, J., McAdam, D., Stearns, L., and Uglow, D. 1980. *The politics of privacy*. New York: Mentor.

Slovic, P. 1987. Perception of risk. *Science* 236:280–285.

Slovic, P. 1997. Trust, emotion, sex, politics, and science: Surveying the risk-assessmentbattlefield. In *Environment, ethics and behavior*, eds. M. Bazerman, D. Messick, A. Tenbrunsel, and K. Wade-Benzoni, pp. 277–313. San Francisco: New Lexington Press.

Stewart, B. 1996. Privacy Impact Assessments. Paper presented to the Privacy Issues Forum, Christchurch, New Zealand, 13 June.

Székely, I., ed. 1991. *Information privacy in Hungary*. Budapest: Hungarian Institute for Public Opinion Research.

Thomas, W. 1928. *The child in America*. New York: Knopf.

Warren, S., and Brandeis, L. 1890. The Right to privacy. *Harvard Law Review* 4(5):193–220.

Westin, A. 1967. *Privacy and freedom*. London: Bodley Head.